AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for automatically negotiating a security protocol, comprising:

receiving a security authorization request to establish a secure connection between an internal node having a first protocol set ~~the internal node being internal to a security-enabled domain,~~ and an external node having a second protocol set, wherein:

(1) the internal node is within a security-enabled domain comprising a centralized distributed directory that maintains security information for a plurality of nodes; and

(2) the external node is not included within the software-based, directory of nodes; ~~the external node being external to the security-enabled domain~~;

comparing the first protocol set associated with the internal node to the second protocol set associated with the external node;

determining that the first node and the second node contain two or more security protocols in common;

selecting a preferred protocol from the two or more security protocols based on transfer speeds associated with the two or more security protocols,

wherein the transfer speeds refer to the speeds that network data can be transferred using the two or more security protocols; and

~~determining a selected protocol from the two or more protocols in common; and~~

automatically establishing a secure connection between the external node and the internal node based on the ~~selected~~ preferred protocol

2. (Original) A method according to claim 1, wherein the external node comprises at least one of a computer and a network-enabled wireless device.

3. (Original) A method according to claim 1, wherein the internal node comprises at least one of a client computer and a server.

4. (Original) A method according to claim 1, wherein the security-enabled domain comprises a distributed directory domain.

5. (Original) A method according to claim 1, wherein the security-enabled domain comprises a certificate-based domain.

6. (Original) A method according to claim 5, wherein the certificate-based domain comprises a Kerberos-enabled domain.

7. (Original) A method according to claim 6, wherein the matching protocol comprises an X.509 certificate.

8. (Original) A method according to claim 1, wherein the security authorization request is generated by the external node.

9. (Previously Presented) A method according to claim 8, wherein the selected protocol is determined based on at least one of a set of criteria, the set of criteria comprising a transfer speed and a bit depth of keys

10. (Original) A method according to claim 1, wherein the security authorization request is generated by the internal node.

11. (Original) A method according to claim 10, wherein the step of receiving the security authorization request is executed by the external node.

12. (Original) A method according to claim 1, further comprising a step of terminating the secure connection when a session between the external node and the internal node is complete.

13. (Canceled).

14. (Original) A method according to claim 1, further comprising a step of selecting a protocol to use in establishing the secure connection when a plurality of matching protocols are found.

15. (Original) A method according to claim 1, further comprising a step of authenticating at least one of the internal node and the external node.

16. (Original) A method according to claim 15, wherein the step of authenticating comprises communicating a certificate to a certificate authority.

17. (Currently Amended) A system for automatically negotiating a security protocol, comprising:

an internal node, the internal node being included within a software-based, distributed directory of nodes, ~~internal to a security-enabled domain~~, the internal node configured to store a ~~having an associated~~ first protocol set comprising one or more security protocols supported by the internal node; ~~and~~

a negotiation engine, the negotiation engine configured for:

(1) receiving a security authorization request to establish a secure connection between the internal node having ~~a~~ the first protocol set and an external node being external to the security-enabled domain, the external node configured to store ~~having~~ a second protocol set comprising security protocols supported by the external node,

(2) comparing the first protocol set associated with the internal node to the second protocol set associated with the external node;

(3) determining that the first protocol set and the second protocol set contain two or more security protocols in common,

(4) selecting a preferred protocol from the two or more security protocols based on at least one of transfer speeds associated with the two or more security protocols and bit depths of one or more encryption keys, wherein:

a) the transfer speeds include the speeds that network data can be transferred using the two or more security protocols, and

b) the bit depths of one or more encryption keys include the number of bits constituting the one or more encryption keys; and

~~(5) determining a selected protocol from the two or more protocols in common, and~~

(6) automatically establishing a secure connection between the external node and the internal node based on the ~~selected~~ preferred protocol.

18. (Original) A system according to claim 17, wherein the external node comprises at least one of a computer and a network-enabled wireless device.

19. (Previously Presented) A system according to claim 17, wherein the selected protocol is determined based on at least one member of a set of criteria, the set of criteria comprising a transfer speed and a bit depth of keys.

20. (Original) A system according to claim 17, wherein the security-enabled domain comprises a distributed directory domain.

21. (Original) A system according to claim 17, wherein the security-enabled domain comprises a certificate-based domain.

22. (Original) A system according to claim 21, wherein the certificate-based domain comprises a Kerberos-enabled domain.

23. (Original) A system according to claim 22, wherein the matching protocol comprises an X.509 certificate.

24. (Original) A system according to claim 17, wherein the security authorization request is generated by the external node.

25. (Original) A system according to claim 24, wherein the security authorization request is received by the internal node.

26. (Original) A system according to claim 17, wherein the security authorization request is generated by the internal node.

27. (Original) A system according to claim 26, wherein the security authorization request is received by the external node.

28. (Original) A system according to claim 17, wherein the negotiation engine terminates the secure connection when a session between the external node and the internal node is complete.

29. (Original) A system according to claim 17, wherein the negotiation engine terminates connection processing when no match between the first protocol set and the second protocol set is found.

30. (Original) A system according to claim 17, wherein the negotiation engine selects a protocol to use in establishing the secure connection when a plurality of matching protocols are found.

31. (Original) A system according to claim 17, wherein at least one of the internal node and the external node authenticates the other.

32. (Original) A system according to claim 31, wherein the authenticating comprises communicating a certificate to a certificate authority.

33-48. (Cancelled)

49. (Currently Amended) One or more tangible computer-readable media having computer-executable instructions embodied thereon, the computer-executable instructions being configured to execute a method for automatically negotiating a security protocol, the method comprising:

receiving a security authorization request to establish a secure connection between an internal node~~, the internal node being internal to a security-enabled domain,~~ and an external node, ~~the external node being external to the security-enabled domain~~ wherein:

(1) the internal node stores a first protocol set identifying one or more security protocols supported by the internal node, and

(2) the external node stores a second protocol set identifying security protocols supported by the external node;

comparing the first protocol set associated with the internal node to the second protocol set associated with the external node;

determining that the first protocol set and the second protocol set contain two or more security protocols in common;

~~determining a selected protocol from the two or more protocols in common; and~~

selecting a preferred protocol from the two or more security protocols based on transfer speeds associated with the two or more security protocols, wherein the transfer speeds refer to the speeds that network data can be transferred using the two or more security protocols; and

automatically establishing a secure connection between the external node and the internal node based on the selected protocol.

50. (Previously Presented) The one or more computer-readable media of claim 49, wherein the external node comprises at least one of a computer and a network-enabled wireless device.

51. (Previously Presented) The one or more computer-readable media of claim 49, wherein the internal node comprises at least one of a client computer and a server.

52. (Previously Presented) The one or more computer-readable media of claim 49, wherein the security-enabled domain comprises a distributed directory domain.

53. (Previously Presented) The one or more computer-readable media of claim 49, wherein the security-enabled domain comprises a certificate-based domain.

54. (Previously Presented) The one or more computer-readable media of claim 53, wherein the certificate-based domain comprises a Kerberos-enabled domain.

55. (Previously Presented) The one or more computer-readable media of claim 54, wherein the matching protocol comprises an X.509 certificate.

56. (Previously Presented) The one or more computer-readable media of claim 49, wherein the step of generating a security authorization request is executed by the external node.

57. (Previously Presented) The one or more computer-readable media of claim 56, wherein the step of receiving the security authorization request is executed by the internal node.

58. (Previously Presented) The one or more computer-readable media of claim 49, wherein the step of generating a security authorization request is executed by the internal node.

59. (Previously Presented) The one or more computer-readable media of claim 58, wherein the step of receiving the security authorization request is executed by the external node.

60. (Previously Presented) The one or more computer-readable media of claim 49, wherein the method further comprises a step of terminating the secure connection when a session between the external node and the internal node is complete.

61. (Canceled).

62. (Previously Presented) The one or more computer-readable media of claim 49, wherein the method further comprises a step of selecting a protocol to use in establishing the secure connection when a plurality of matching protocols are found.